presented by

American Megatrends

PreBoot Provisioning Solutions with UEFI

UEFI Spring Plugfest – May 18-22, 2015

Presented by Zachary Bobroff (AMI)

Agenda

- Introduction
- Building on Top of the UEFI Specification
- Expanding Further
- Call to Action

PreBoot Provisioning Solutions with UEFI

Introduction

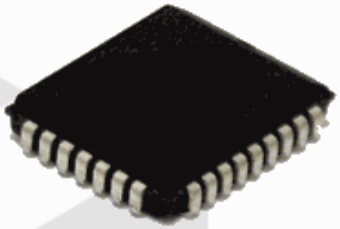
Current Challenges for Provisioning

- UEFI systems need to be configured to meet datacenter and corporate policies
- Systems crash in the field and current recovery mechanisms don’t always fit
- As OS and firmware updates come out, they need to be quickly and effectively deployed globally
- Provisioning utilities on a disk are susceptible to corruption and malicious software

Why cant a feature rich provisioning be developed for use in firmware?

Firmware Based Provisioning

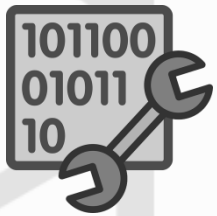
- Firmware based provisioning is already included in the flash part
  - External media provisioning still needs factory provisioning
- Firmware has access to information and interfaces that is not available to external applications
- As the root of trust, the firmware is the most secure part of a platform



UEFI 2.5 Makes it Easier

- FMP has been expanded to include support for updating the firmware of any device on a system in a common manner

- System configuration data has been expanded so configuration data layout can be known outside of the firmware itself



- HTTP support has been expanded to an entire client stack to allow full network access and even access to the internet

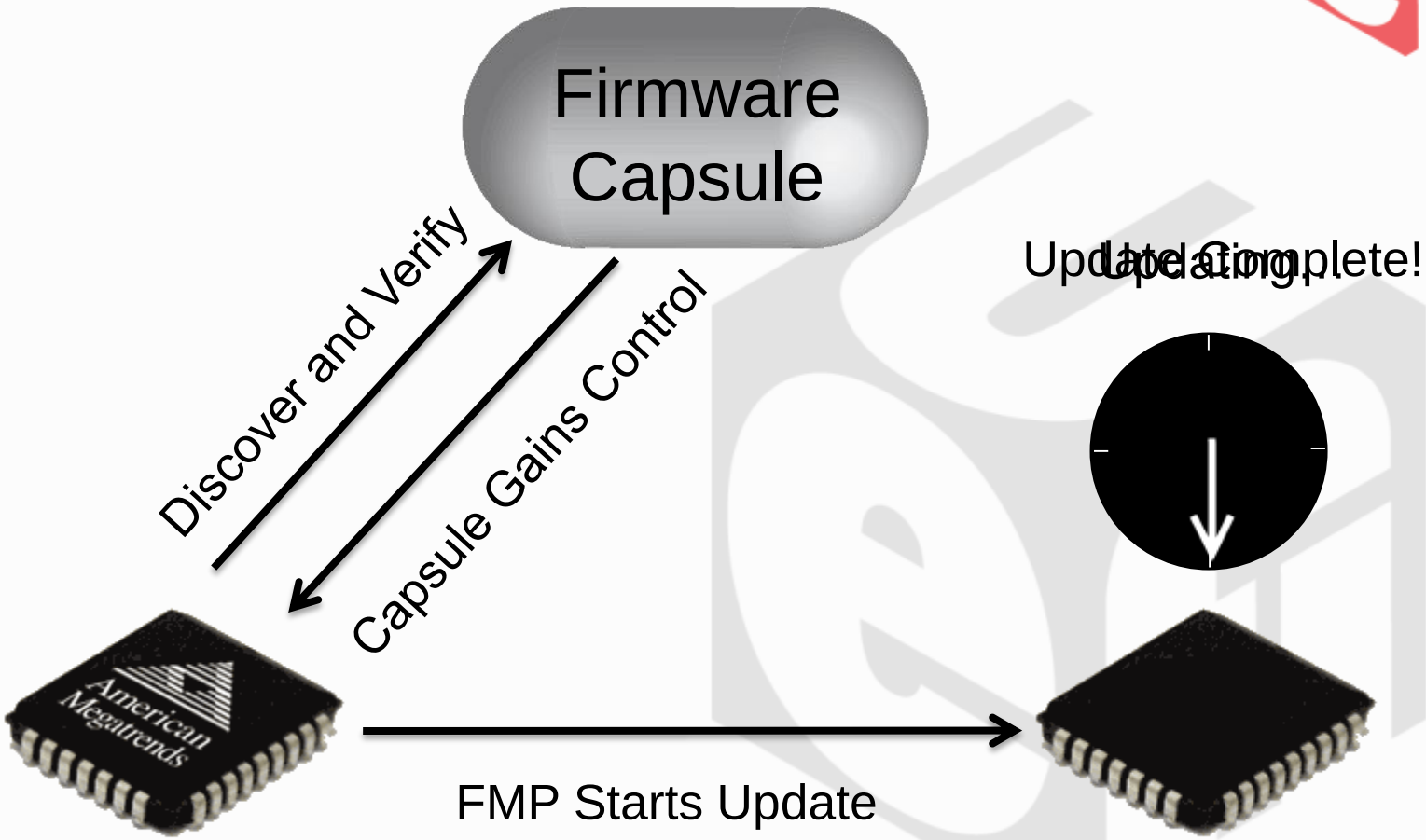
PreBoot Provisioning Solutions with UEFI

Building on Top of the UEFI Specification

Firmware Management Protocol (FMP)

- Capsules can now be code and data!
  - Saving space and boot time for the firmware
- FMP allows external devices to manage the security of their own firmware
- Updating via a capsule is the most secure method available today

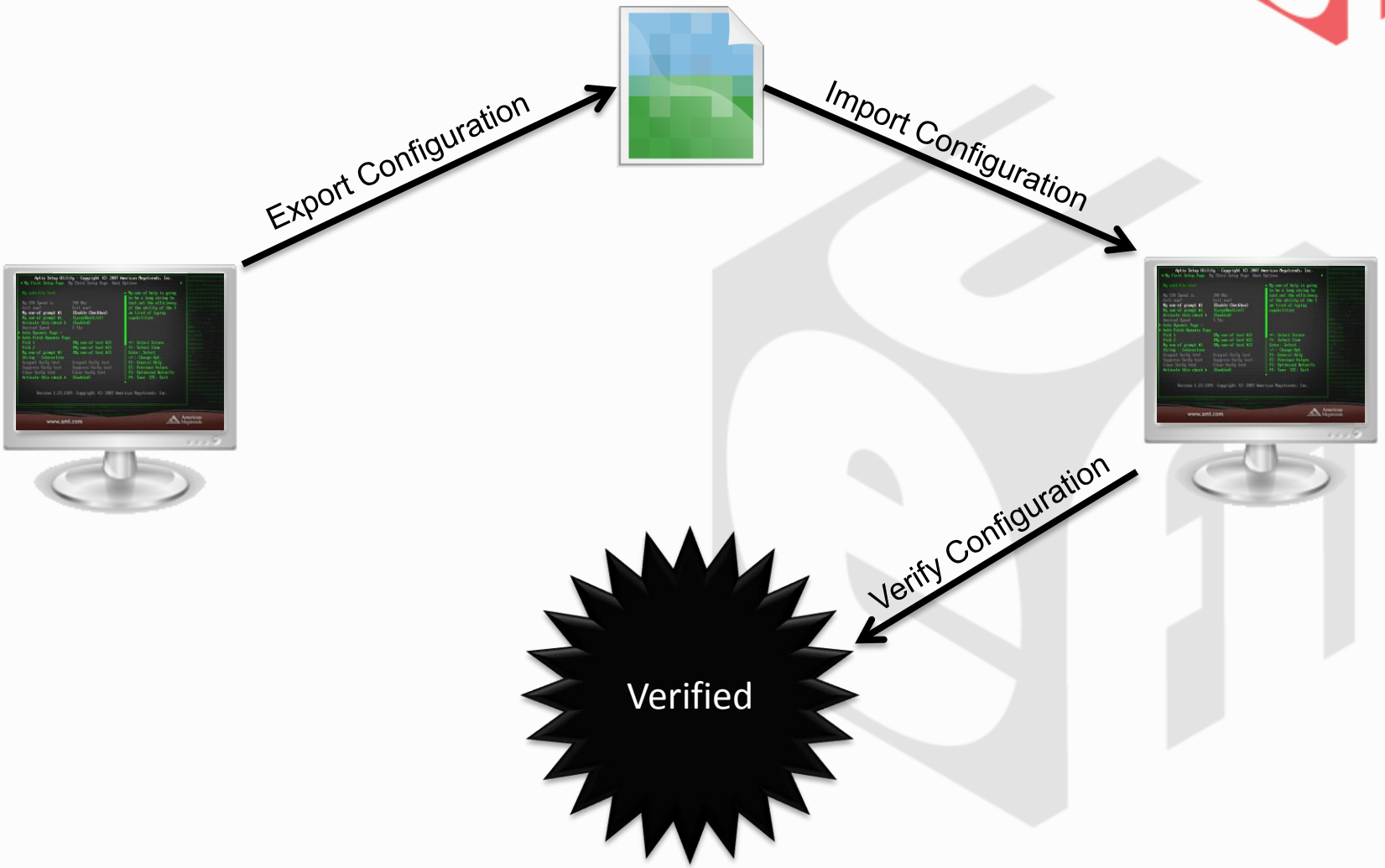
FMP Update in Action



System Configuration Data

- X-UEFI language has allowed a common mapping of configuration options to a master list
- New mappings allows:
  - Migration of current configuration during firmware updates
  - Current configuration can be migrated to other systems more easily
  - Common look and feel for different systems
  - External agents can modify specific settings through OEM proprietary methods
- OpRom vendors should provide similar mappings

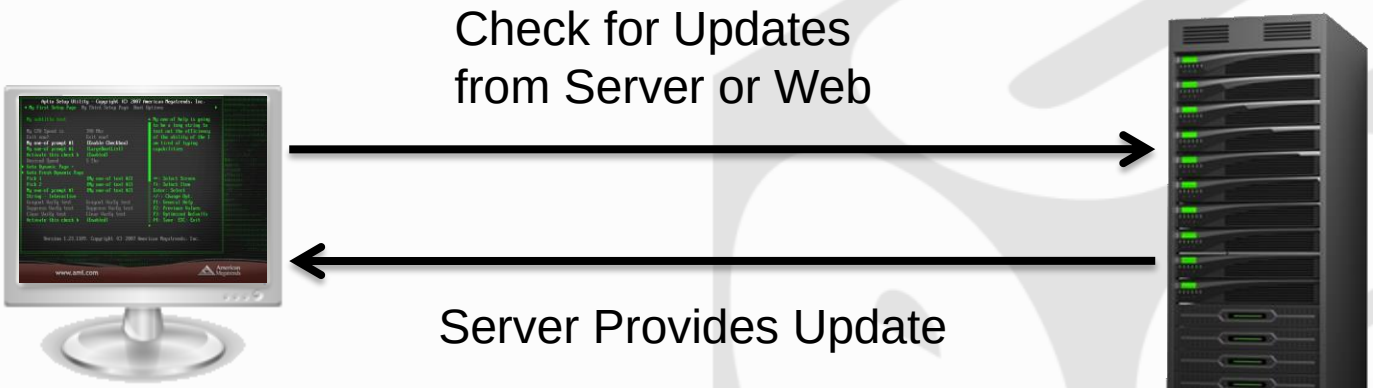
System Configuration Data Migration



HTTP Support

- UEFI 2.5 has added a complete client side HTTP stack allowing network access to:
  - Do system firmware updates
  - Check for any needed system configuration changes
  - Download any OS images or updates
- Server for providing images can be located in a datacenter, corporation or by the ODM
  - Throw away the recovery CD and recovery partition!

HTTP Update BIOS/Configuration/OS



Advanced Networking Support

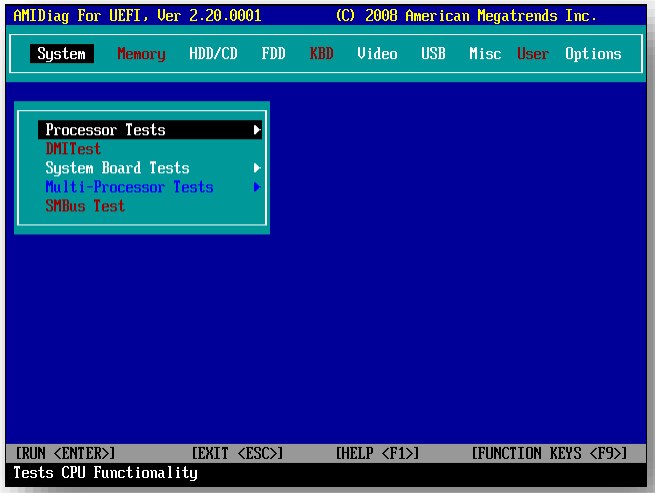
- For the security conscious, UEFI's HTTP support can be expanded
- VPNs can be setup through IPSec
- Services like KMS implemented on top of advanced UEFI network interfaces such as HTTP and TLS will provide an implementation that is free from packet snooping

PreBoot Provisioning Solutions with UEFI

Building Further

System Diagnostics

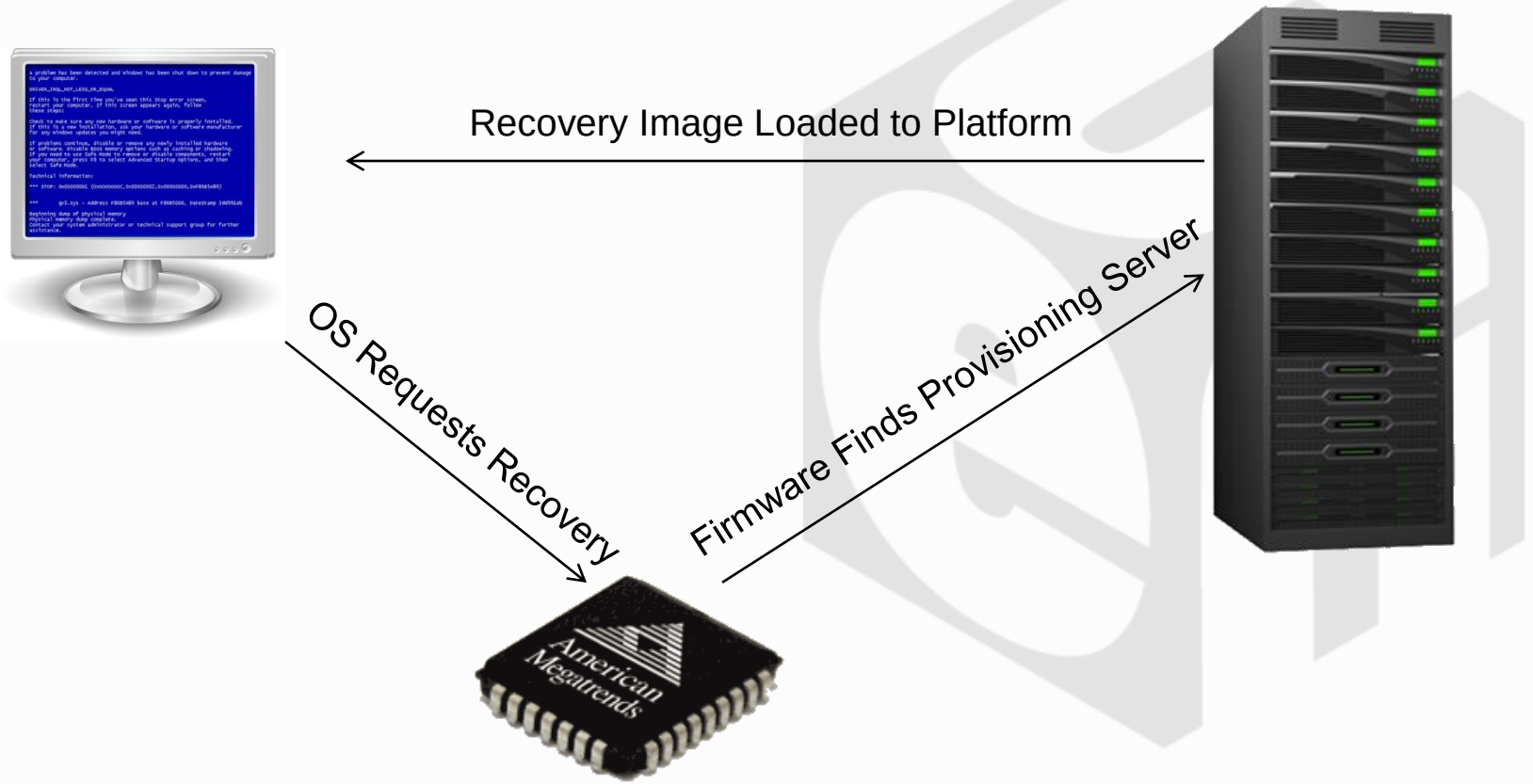
- UEFI provides many interfaces to create diagnostics tools



IHVs should be providing the EFI_DRIVER_DIAGNOSTICS2_PROTOCOL to automatically extend platform diagnostics support

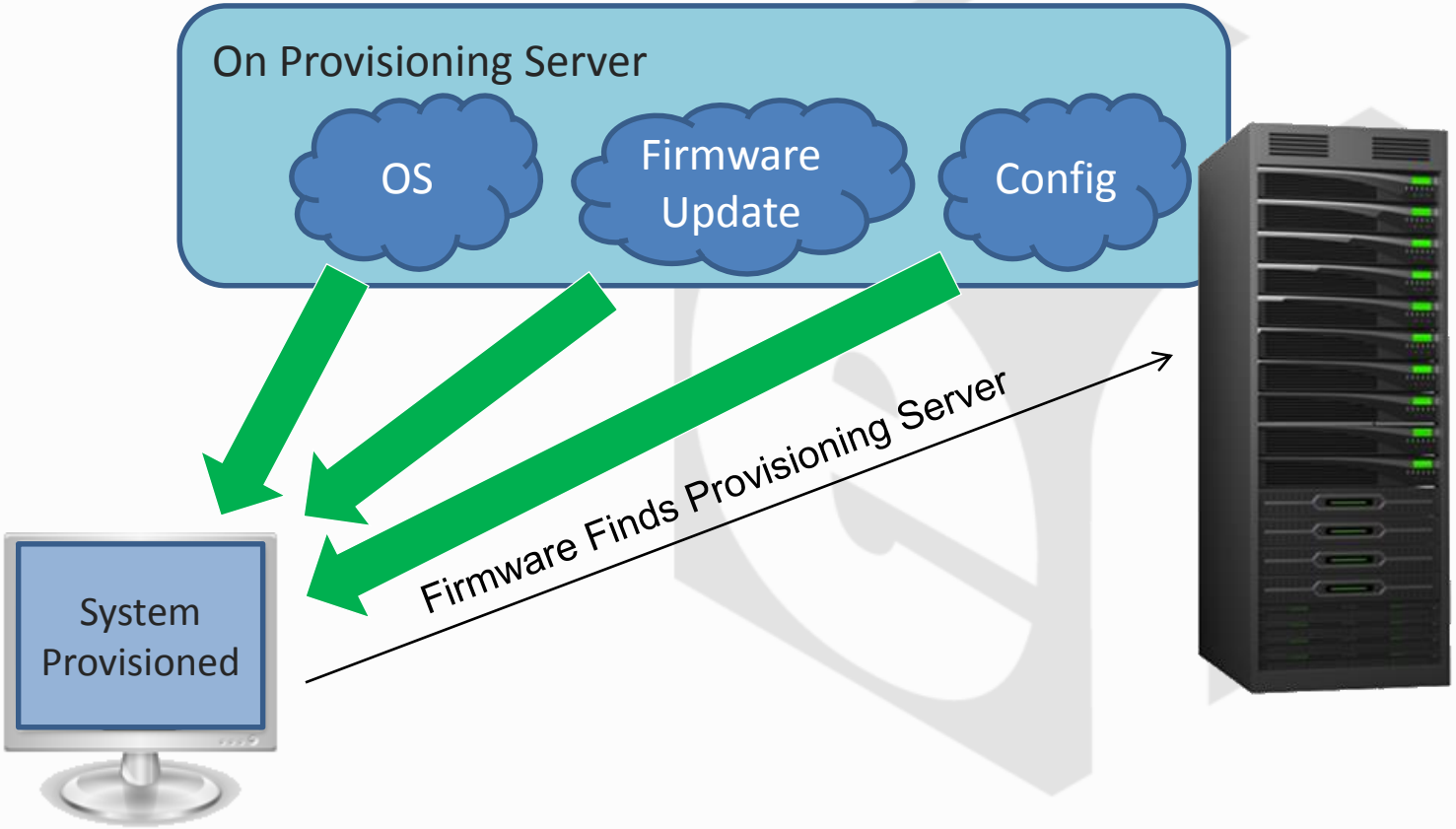
System Auto-Recovery

- OS can inform firmware of crash to auto-initiate recovery though EFI_OS_INDICATIONS_START_PLATFORM_RECOVERY bit



System Auto-Provision

- As systems arrive from factory they can auto-provision at the customer site



PreBoot Provisioning Solutions with UEFI

Call to Action

Call to Action

- Add-on card vendors and third party HW vendors should provide FMP and diagnostics capabilities
- All firmware that uses system configuration methods should produce x-UEFI mappings
- OEMs should build industry ready solutions for configuration, provisioning, recovery and diagnostics
  - OEMs need to be solution providers!

Thanks for attending the
UEFI Spring Plugfest 2015

For more information on the Unified EFI Forum and UEFI Specifications, visit http://www.uefi.org

presented by